Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): NAI1P317/01.185.01

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed name Erica L. Farlow

Application Number	Filed
10/091,645	03/05/2002

First Named Inventor: H. Wu et al.

Art Unit	Examiner
2132	Homayounmehr, F.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 41,429
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

Signature

Kevin J. Zilka

Typed or printed name

(408) 971-2573

Telephone number

1/12/06

Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

REMARKS

The Examiner has rejected Claims 21 and 22 under 35 U.S.C. 112, first paragraph, as not being enabled. With respect to Claim 21, the Examiner has questioned the exact implication of the "frame_context_pointer_position" limitations. With respect to Claim 22, the Examiner has stated that Page 12 of the specification only mentions the incision of "frame_tcp_bridge," "frame_udp_bridge," "frame_ip_bridge," and "frame_http_bridge," but does not give a description of the specific functionality of such elements.

Applicant respectfully asserts that Page 12 of applicant's disclosure describes the form the API's may take, or, in other words, defines the form that the API takes. Thus, according to the claims, the API is defined according to "frame_context_pointer_position" (Claim 21) which includes "frame_tcp_bridge; frame_udp_bridge; frame_ip_bridge; and frame_http_bridge" (Claim 22).

The Examiner has rejected Claims 1-19 under 35 U.S.C. 102(e) as being anticipated by or, in the alternative, unpatentable under 35 U.S.C. 103(a) as being obvious over Vaidya (U.S. Patent No. 6,279,113) in view of Porras (U.S. Patent Application No. 2003/0101358). Applicant respectfully disagrees with such rejection.

With respect to each of the independent claims, and specifically applicant's claimed "intrusion detection device separate from the data monitoring device," the Examiner has argued, in the latest Office Action dated 11/30/2005, that applicant's claimed "intrusion detection device separate from the data monitoring device" is only separate in functionality. Applicant respectfully points out page 7, line 14-page 8, line 6, along with associated Figure 1, which clearly shows that the network analysis and data monitoring device 16 and the intrusion detection device 14 are separate devices, and not merely that they perform separate functionality, as the Examiner contends.

The Examiner has also argued that Vaidya does not limit his invention to one processor only. In making such an assertion, the Examiner has referenced Figure 4, items 36, 34 and 38 as being separate modules to perform separate functionalities. Applicant respectfully asserts that Figure 4 only discloses modules that work with the virtual processor, but not that such modules are separate processors. Thus, applicant respectfully asserts that the only processing device in Vaidya is the virtual processor. Furthermore, the modules relied on by the Examiner do not provide the separate functionality claimed by applicant, namely "captur[ing] data passing through the network," "perform[ing] intrusion detection," etc.

Still yet, the Examiner has argued that Vaidya performs the functionality of applicant's data monitoring device and intrusion detection device in item 36, but that such functionality is separate as shown in item 40. Applicant respectfully asserts that item 40, the register cache, "temporarily stores information extracted from a data packet which determines which signature profile(s) will be accessed from the signature profile memory 39." Clearly, such register cache that only extracts information from data packets does not meet applicant's claimed "data monitoring device," which specifically "capture[s] data passing through the network," "monitor[s] network traffic," "decode[s] protocols for grouping packets into different protocol presentations and assembling the packets into high level protocol groups," and "analyze[s] received data," in the manner claimed by applicant. Thus, the functionality of items 36 and 40, as relied on by the Examiner, does not meet applicant's specific claim language.

Furthermore, the Examiner has argued that Vaidya's claim 1, which claims a method of detecting intrusion attempts, is broken down into several steps, including monitoring network traffic and network intrusion. Applicant emphasizes that merely claiming separate steps does not meet applicant's separate devices, as claimed. In addition, simply claiming monitoring network traffic, as in Vaidya, does not meet applicant's specifically claimed functionality of a data monitoring device that exceeds beyond monitoring network traffic, as excerpted above.

Applicant again respectfully asserts that the applicant's arguments made in the Office Action dated 10/12/2005 on page 7, paragraph 4-page 9, paragraph 1 clearly show the distinction between Vaidya and applicant's specific claim language.

With respect to applicant's claimed technique "wherein the application program interfaces allow the intrusion detection device to leverage the separate data monitoring device, by allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and by allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device," the Examiner has argued that such claim language in addition to the specification does not point out any advantage in separation of the intrusion detection device and the data monitoring device. In response, applicant points out page 8, lines 3-6 which states that the components, including the intrusion detection device and the network analysis and data monitoring device can perform dual simultaneous functions, etc. which allows for efficient detection of intrusions in high-speed network traffic.

The Examiner has also argued that such aforementioned claim language would have been obvious and well known to a person skilled in the art, and noted Porrass in such regard. Specifically, the Examiner has argued that the motivation to use APIs in order to build the intrusion detection system would have been to take advantage of an already prepared and well tested element to perform part of the required functionality. Applicant respectfully asserts that the alleged obviousness of utilizing APIs does not make applicant's specific claim language obvious, since applicant does not merely claim using APIs, but instead specifically claims "allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and...allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device." Thus, each device, as claimed by applicant, is allowed to call API's with specific separate

functionality such that the intrusion detection device is allowed to leverage the separate data monitoring device. These claimed features are simply non-existent in both Vaidya and Porrass.

With respect to the 102 rejection, the Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

With respect to the 103 rejection, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,*947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991). Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references fail to teach or suggest all of the claim limitations, as noted above.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.